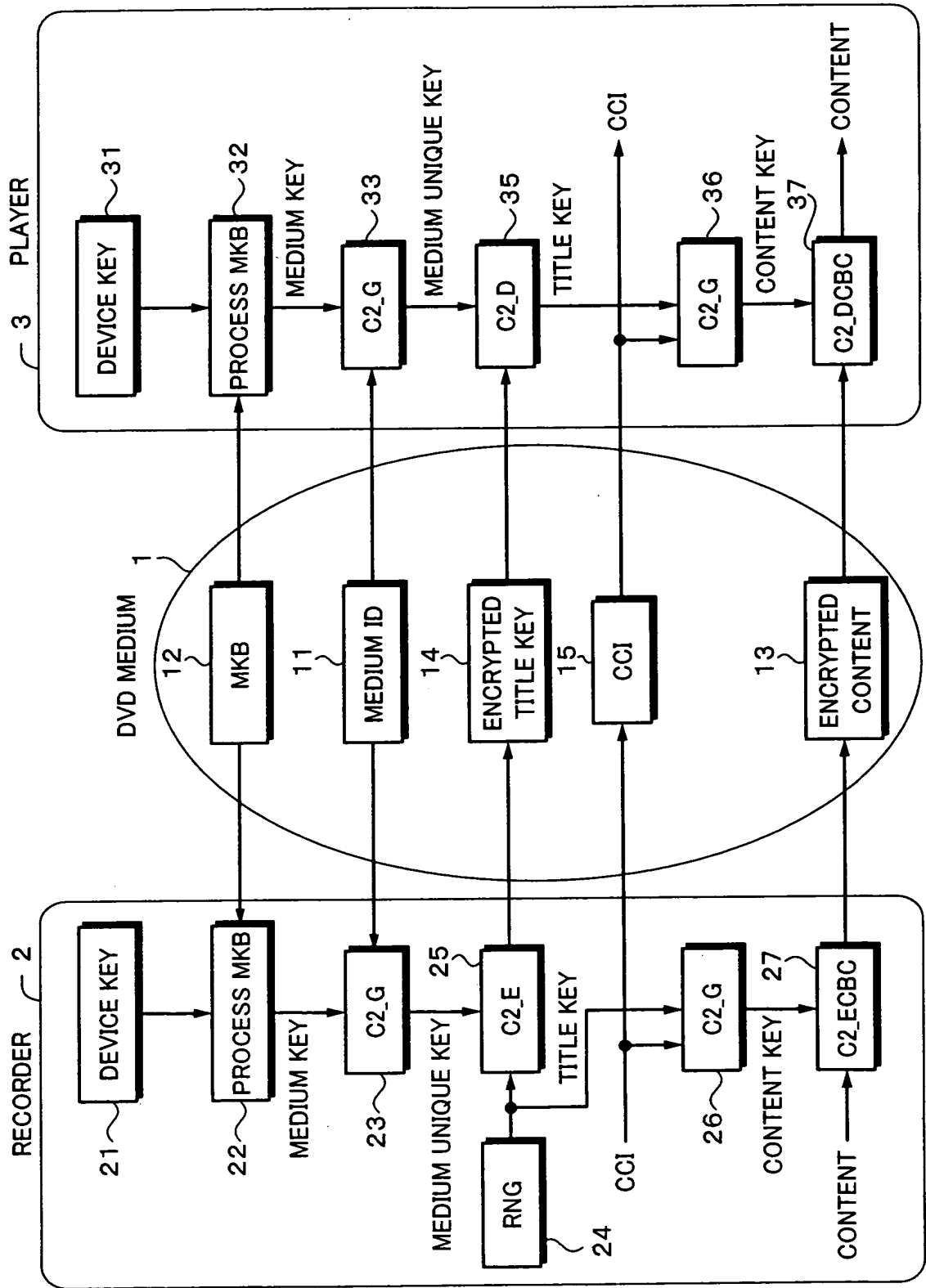
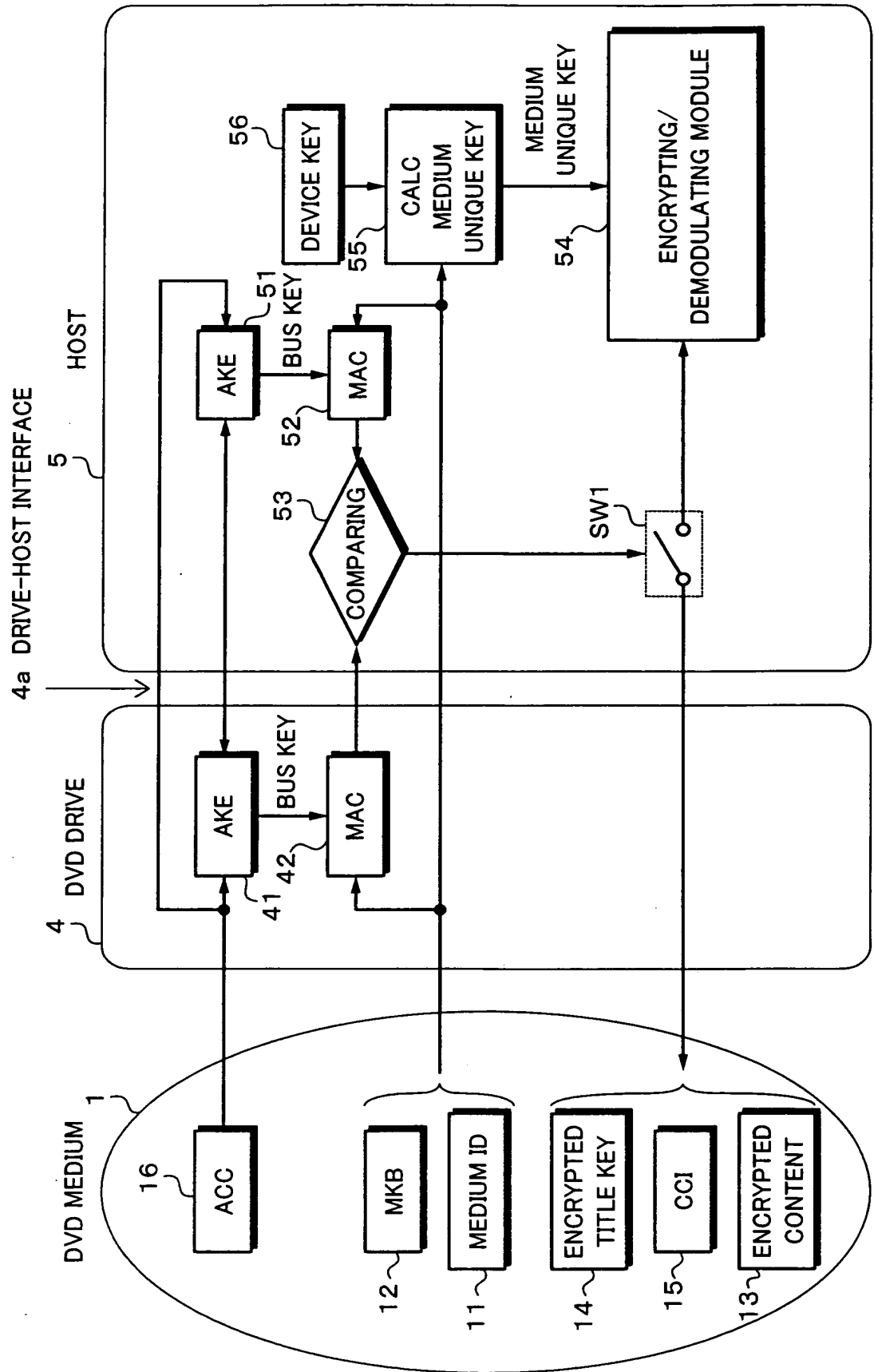


Fig. 1



10/505175

Fig. 2



10/505175

Fig. 3

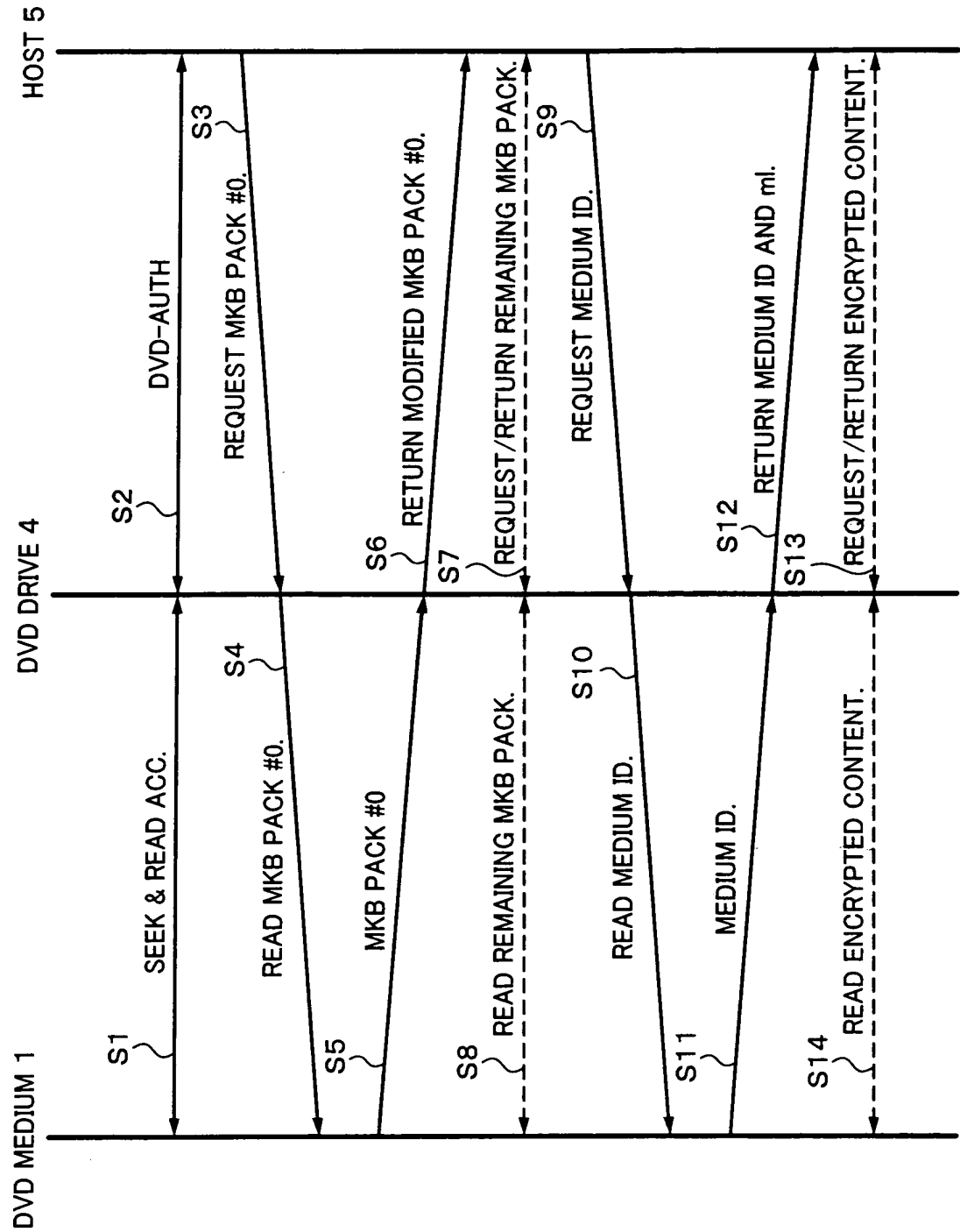


Fig. 4

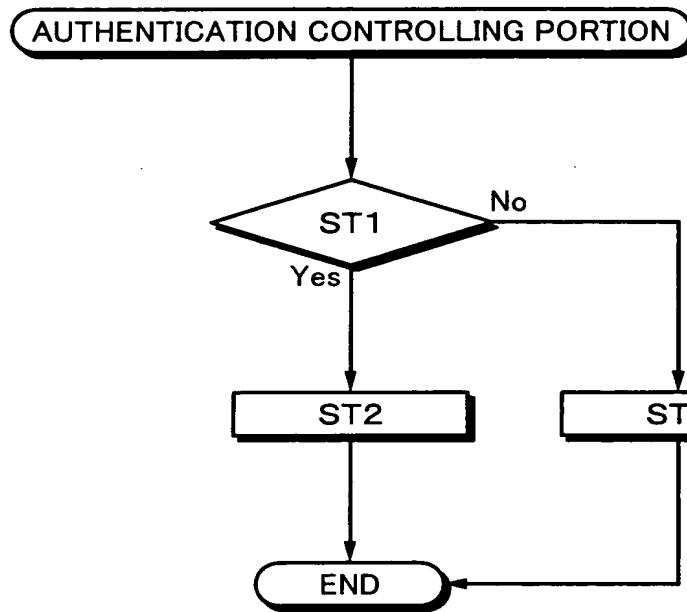


Fig. 5

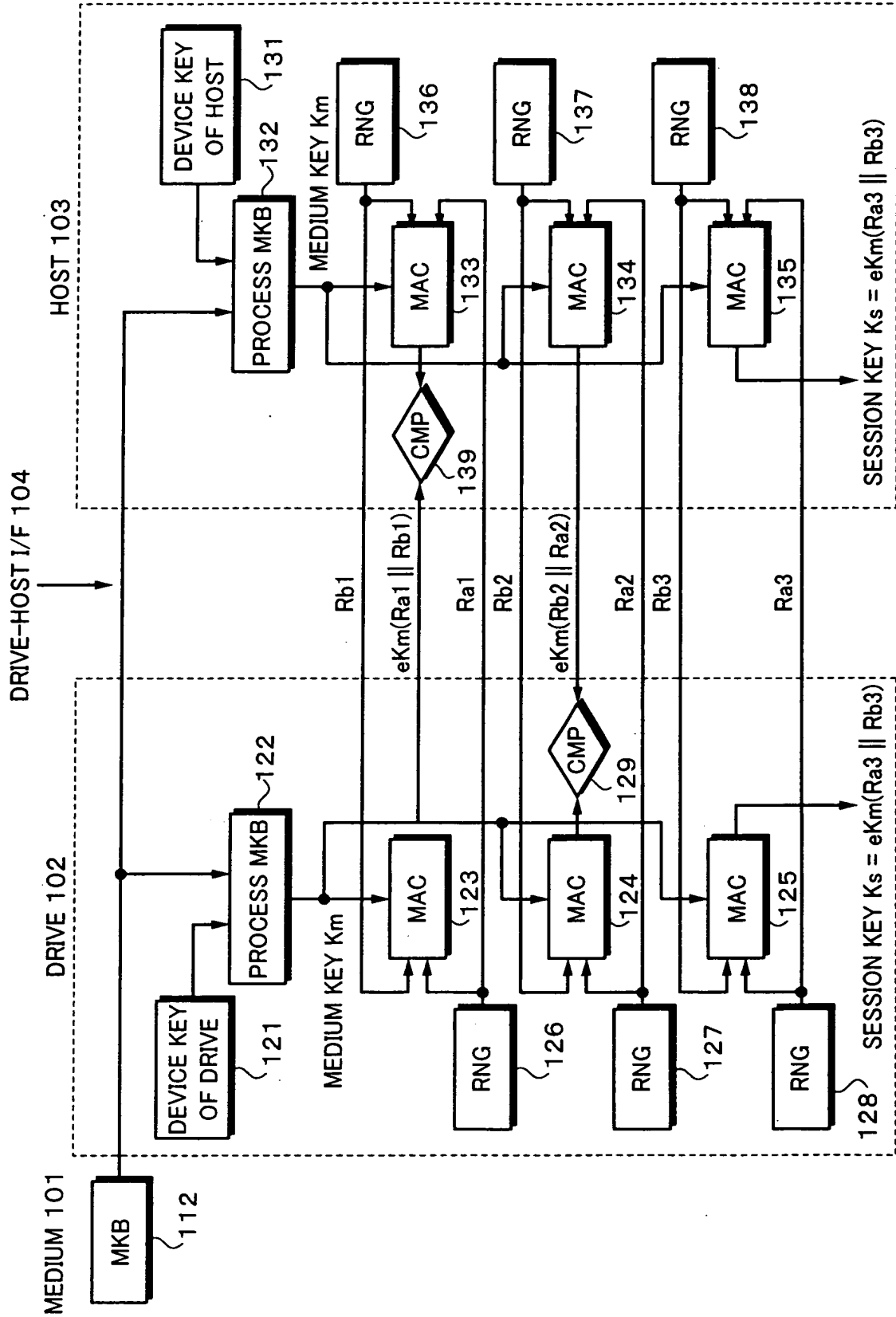
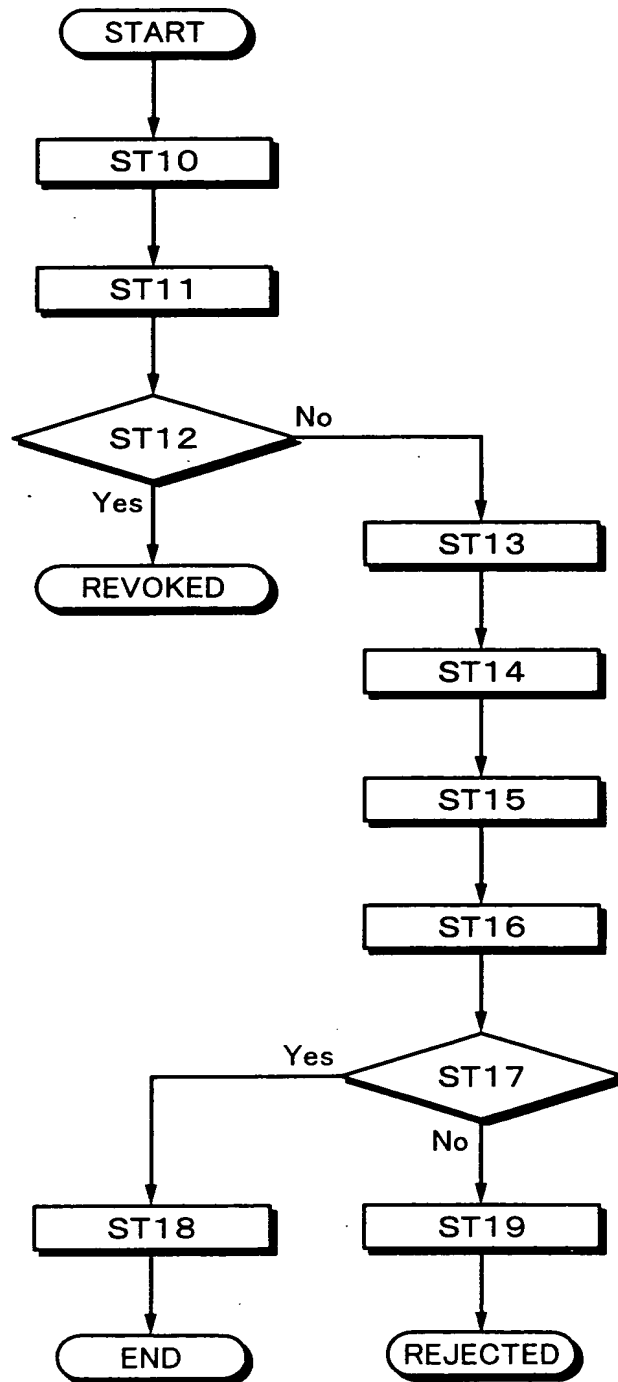


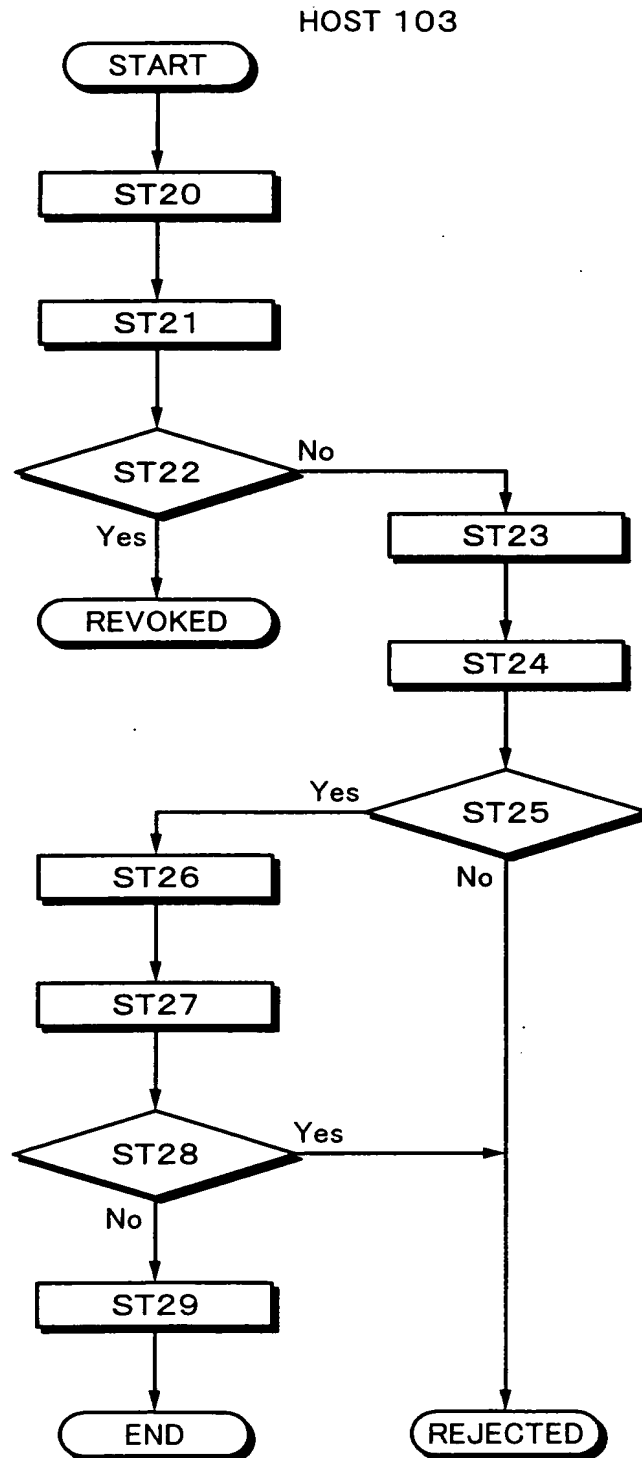
Fig. 6

DRIVE 102



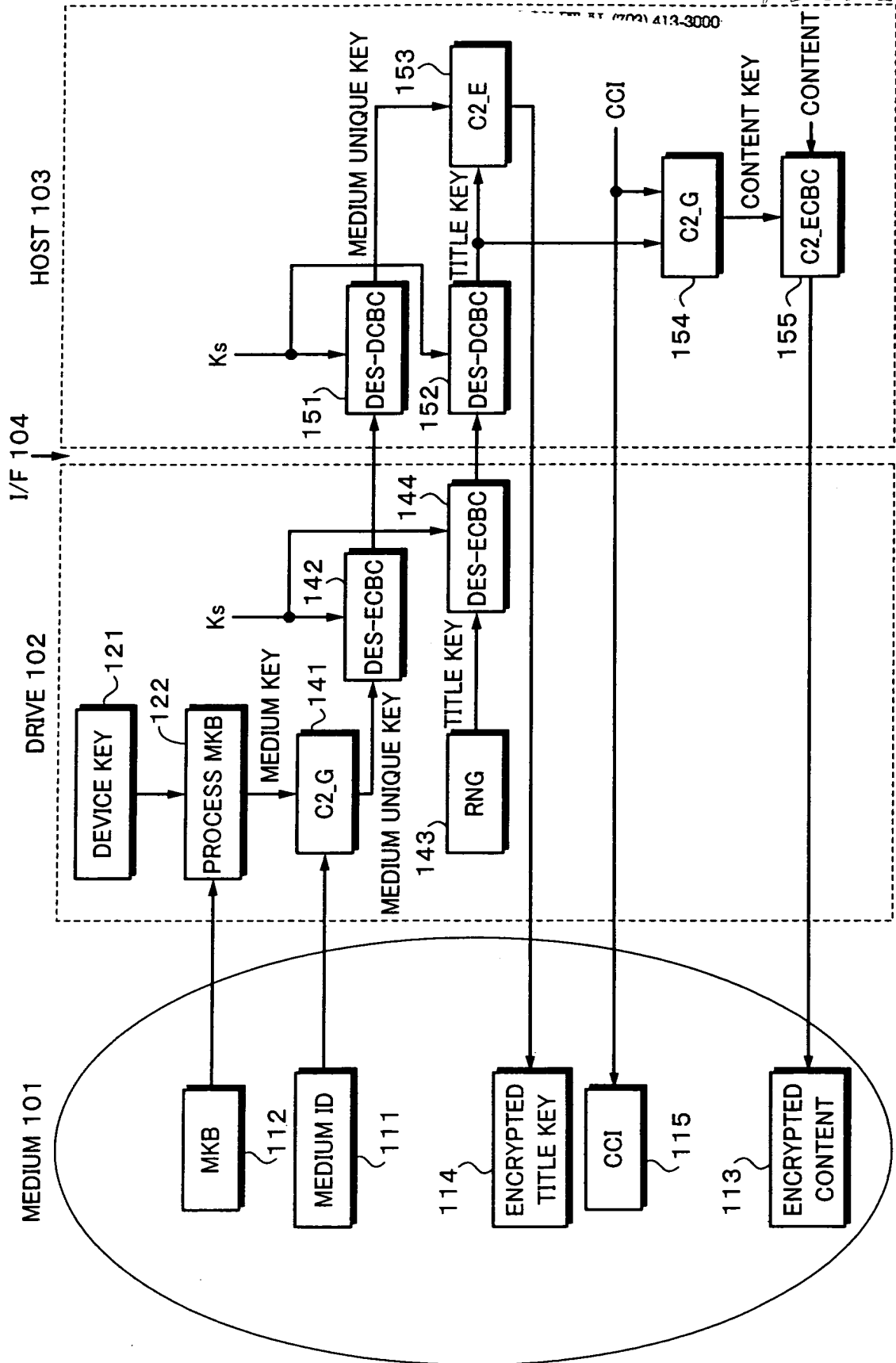
10/505175

Fig. 7



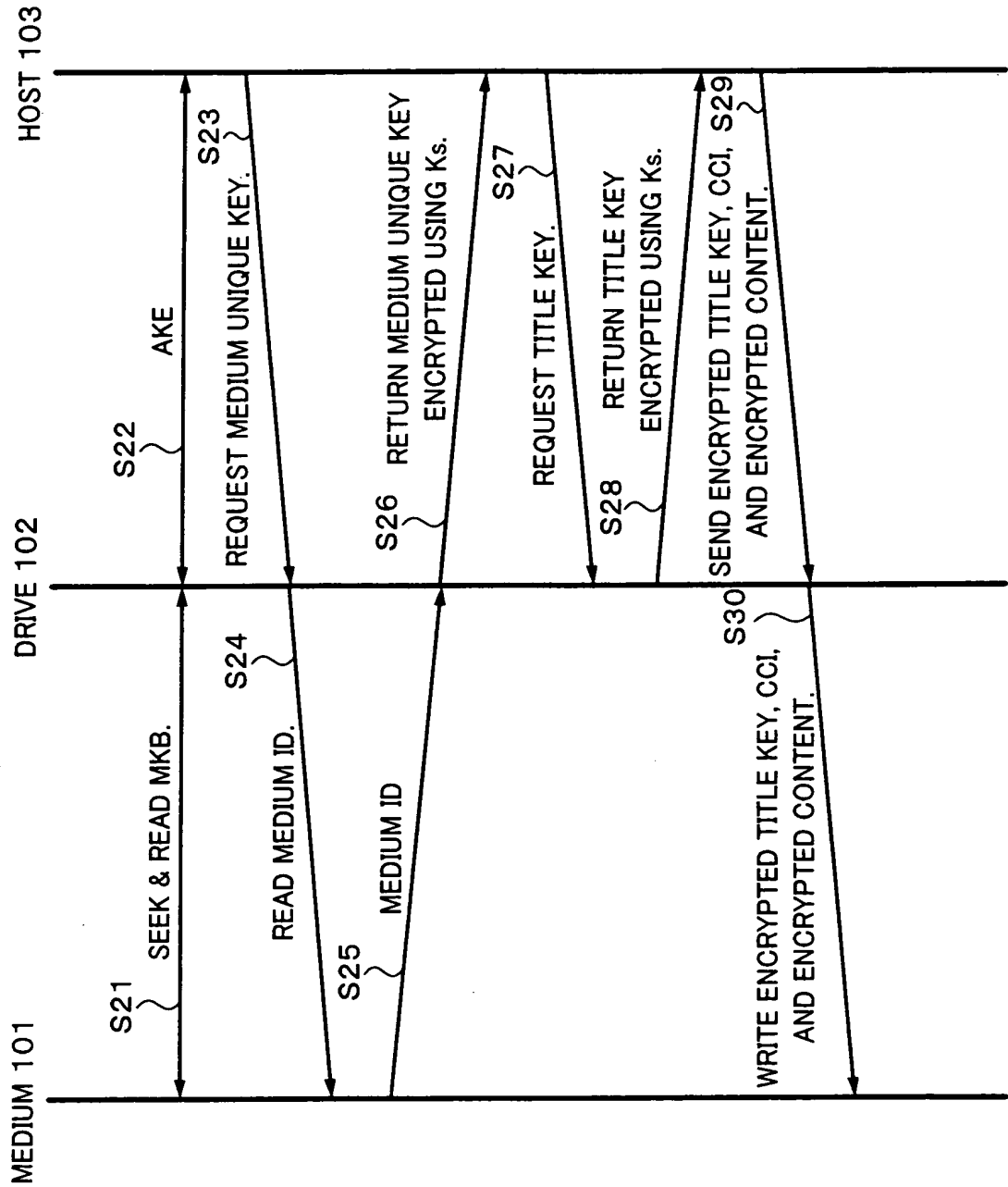
10/505175

Fig. 8



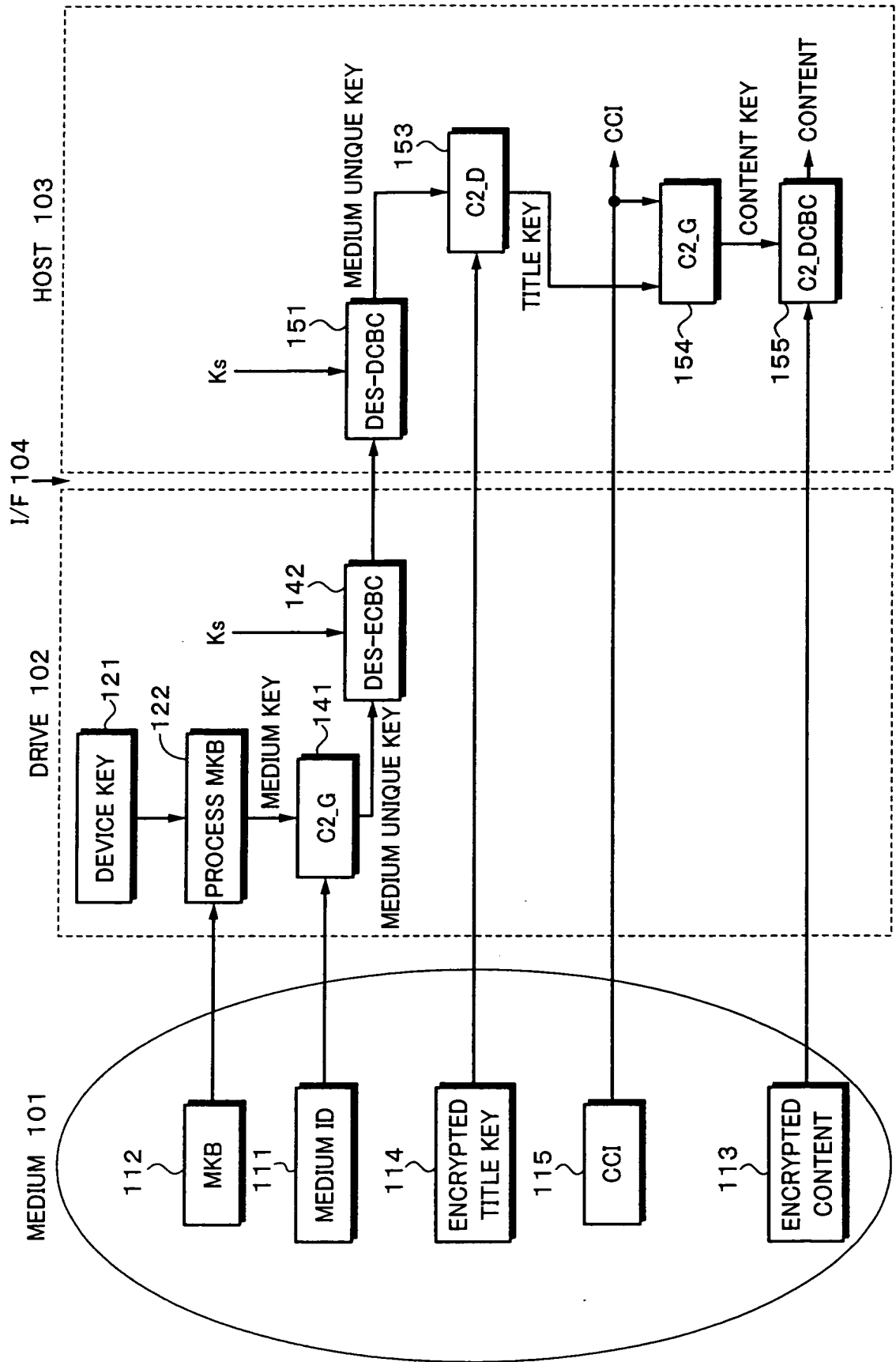
10/505175

Fig. 9



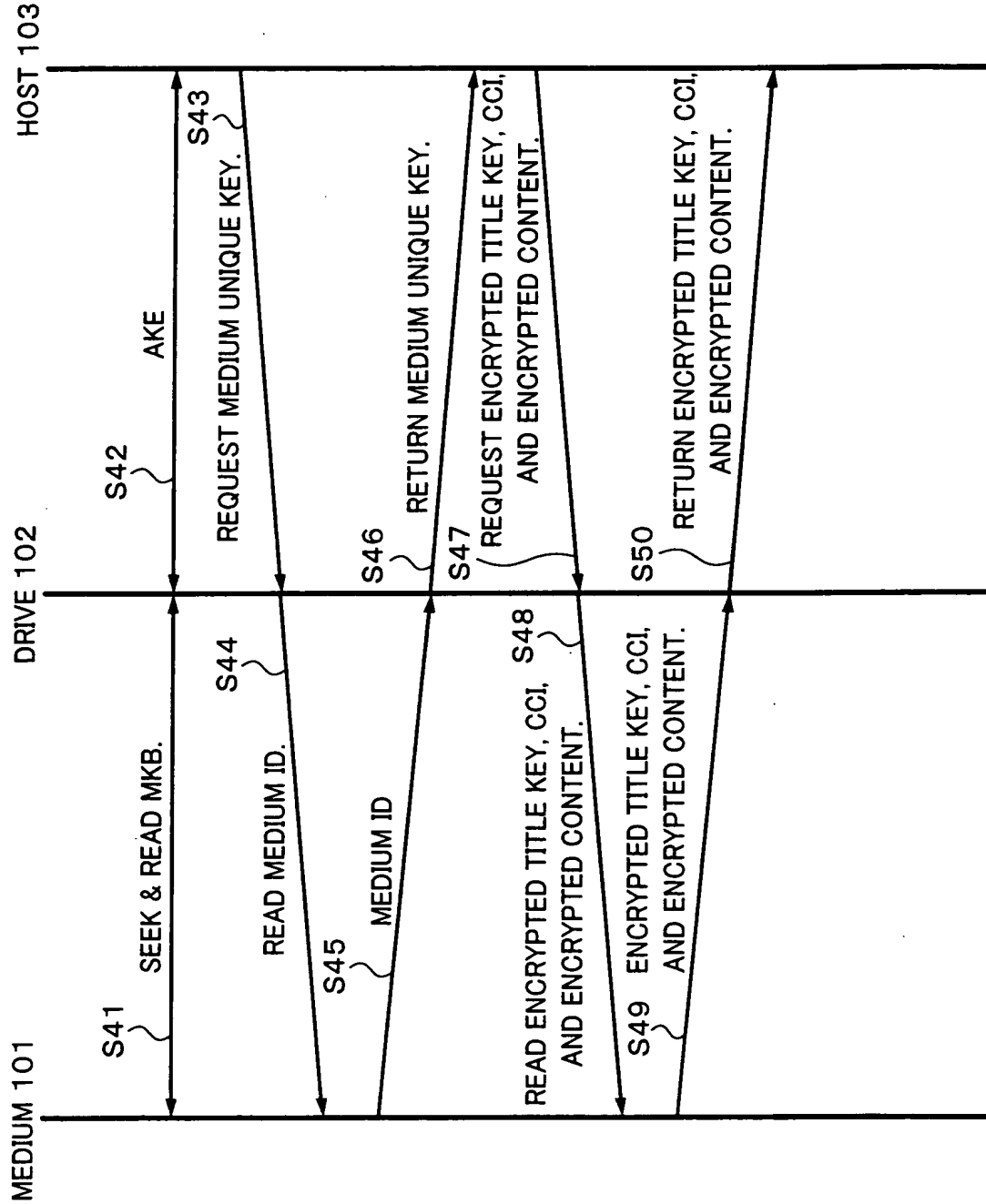
10/305175

Fig. 10



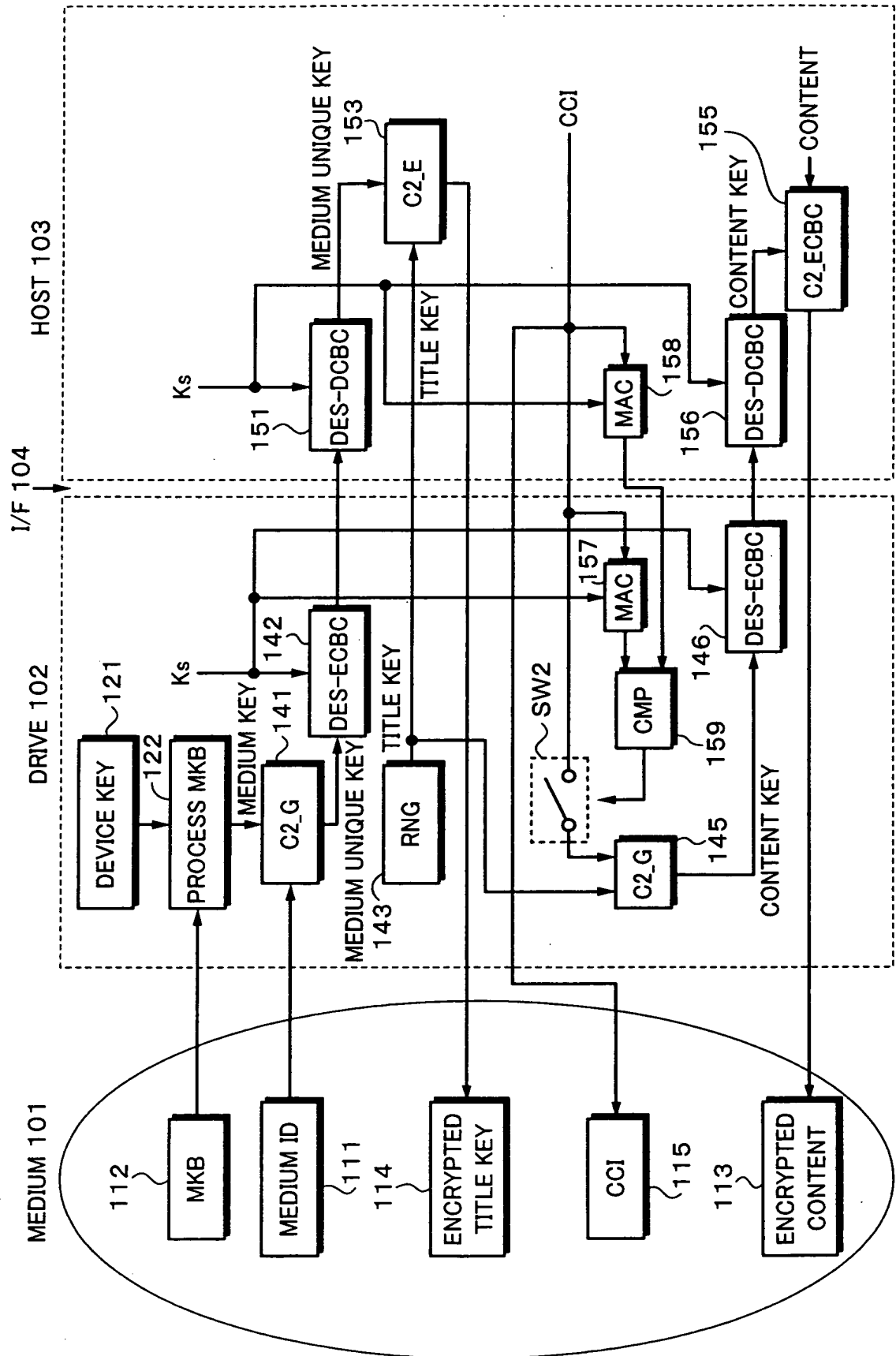
10/505175

Fig. 11



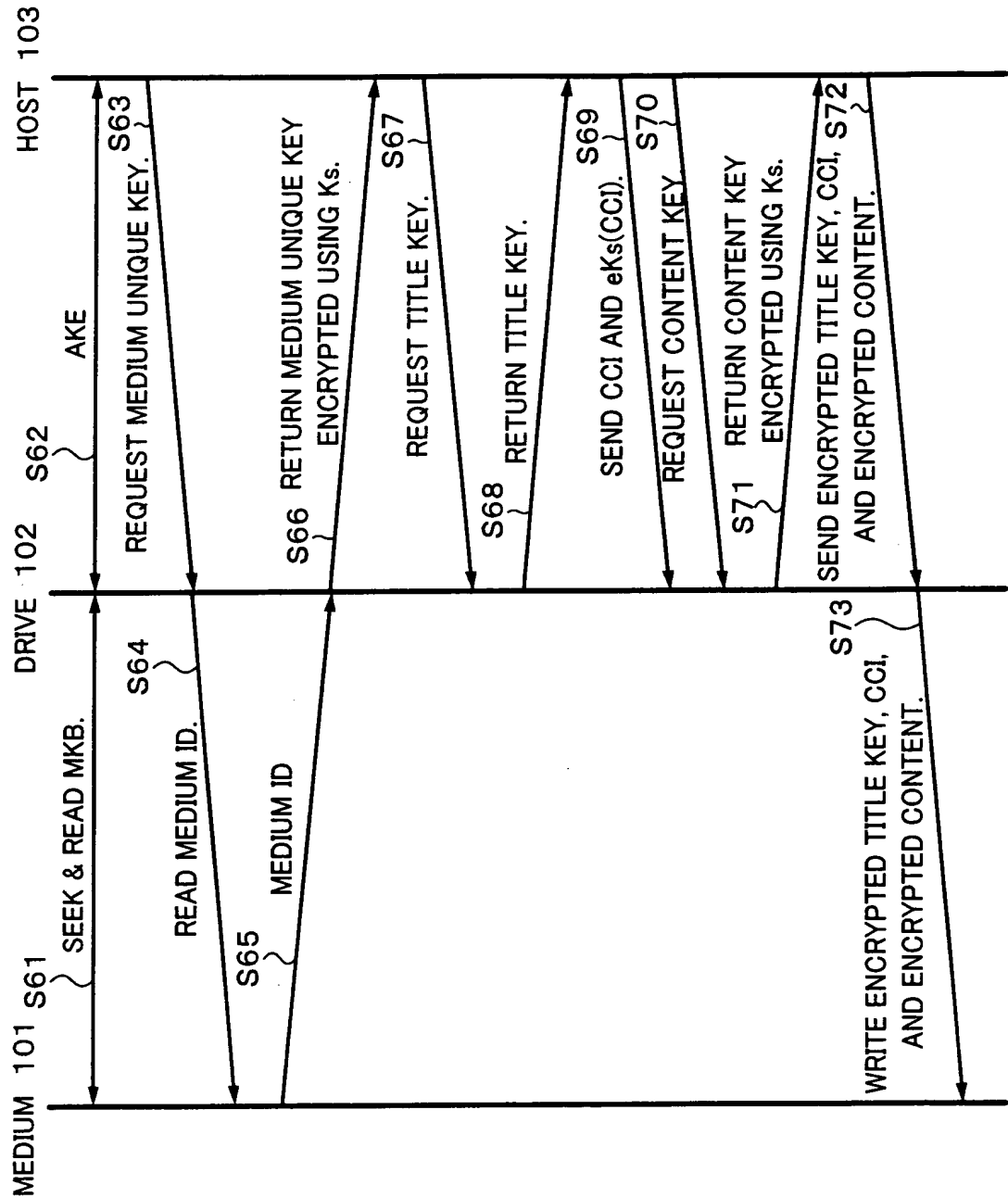
10/505175

Fig. 12



10/505175

Fig. 13



10/505175

DESCRIPTION OF REFERENCE NUMERALS

1	DVD MEDIUM
2	RECORDER
3	PLAYER
4	DVD DRIVE
4a	INTERFACE
5	HOST
11	MEDIUM ID
12	MEDIUM KEY BLOCK (MKB)
13	ENCRYPTED CONTENT
42, 52	MAC CALCULATING BLOCK
46	DEVICE KEY
46a	FIRST HALF PORTION OF DEVICE KEY
47	DES ENCRYPTOR
48	MEDIUM UNIQUE KEY CALCULATING BLOCK
49, 49a	DES ENCRYPTOR
49b	DES DECRYPTOR
53	COMPARING PORTION THAT COMPARE MACS
54	ENCRYPTING/DECRYPTING MODULE
55	MEDIUM UNIQUE KEY CALCULATING BLOCK
101	MEDIUM
102	DRIVE
103	HOST
104	INTERFACE
121	DEVICE KEY OF DRIVE

10/505175

122 PROCESS MKB

123, 124, 125 MAC CALCULATING BLOCK OF DRIVE

126, 127, 128 RANDOM NUMBER GENERATOR OF DRIVE

129 COMPARING

131 DEVICE KEY OF HOST

132 PROCESS MKB

133, 134, 135 MAC CALCULATING BLOCK OF HOST

136, 137, 138 RANDOM NUMBER GENERATOR OF HOST

139 COMPARING

141, 154 C2_G

142, 144 DES ENCRYPTOR

143 RANDOM NUMBER GENERATOR

151, 152, 156 DES DECRYPTOR

153 C2_E

155 C2_EBC

157, 158 MAC CALCULATING BLOCK

159 COMPARING

ST1 MAC CALCULATED VALUES MATCH ?

ST2 TURN ON SWITCH.

ST3 TURN OFF SWITCH.

ST10 REPORT KEY (MKB)

ST11 CALCULATE MEDIUM KEY Km.

ST12 REVOKED ?

ST13 RECEIVE (Rb1, Rb2).

ST14 RETURN (eKm(Ra1 || Rb1), Ra1).

10/505175

ST15 RETURN (Ra2, Ra3).
ST16 RECEIVE (eKm(Rb2 || Ra2), Rb3).
ST17 SAME MAC ?
ST18 SESSION KEY CONFIRMED (eKm(Ra3 || Rb3)
ST19 RETURN (ERROR)
ST20 REPORT KEY (MKB)
ST21 CALCULATE MEDIUM KEY Km.
ST22 REVOKED ?
ST23 SEND KEY (Rb1, Rb2).
ST24 REPORT KEY (eKm(Ra1 || Rb1), Ra1)
ST25 SAME MAC ?
ST26 REPORT KEY (Ra2, Ra3)
ST27 SEND KEY (eKm(Rb2 || Ra2), Rb3)
ST28 ERROR ?
ST29 SESSION KEY CONFIRMED (eKm(Ra3 || Rb3))